★DEBP T01 2000-330102/29 ★DE 19847941-A1

Common cryptographic key establishment method for subscribers involves successively combining two known secret values into a new common value throughout using Diffie-Hellmann technique

DEUT TELEKOM AG 1998.10.09 1998DE-1047941

W01 (2000.04.13) H04L 9/30

Novelty: The method involves using the Diffie-Hellmann or DH technique. A leaf of a binary structured tree with exactly n leaves and depth $\log_2 n$ is allocated to each of the n subscribers (A,B,C). A secret value is generated for each subscriber, and is associated with the relevant leaf. Secret values are established successively towards the tree root for all nodes of the tree, in which two known values are always combined into a new common value. This is done throughout using the DH technique, and is associated with a common node so that the last node (KW), and hence the root, contains the common key for all subscribers.

Use: For establishing a common cryptographic key for subscribers to guarantee the security of messages to be transmitted to the subscribers exclusively over insecure communications channels.

Advantage: Enables subscribers to be removed from or added to the key list even after establishing the group key without great cost.

Description of Drawing(s): The drawing illustrates the working principle of the method and a tree structure for three subscribers

Subscribers A,B,C

Nodes K1,KW

(8pp Dwg.No.1/5)

N2000-248435

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 47 941 A 1**

(51) Int. Cl.[7]: H 04 L 9/30

(21) Aktenzeichen: 198 47 941.7
(22) Anmeldetag: 9. 10. 1998
(43) Offenlegungstag: 13. 4. 2000

DE 198 47 941 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Schwenk, Jörg, Dr., 64807 Dieburg, DE

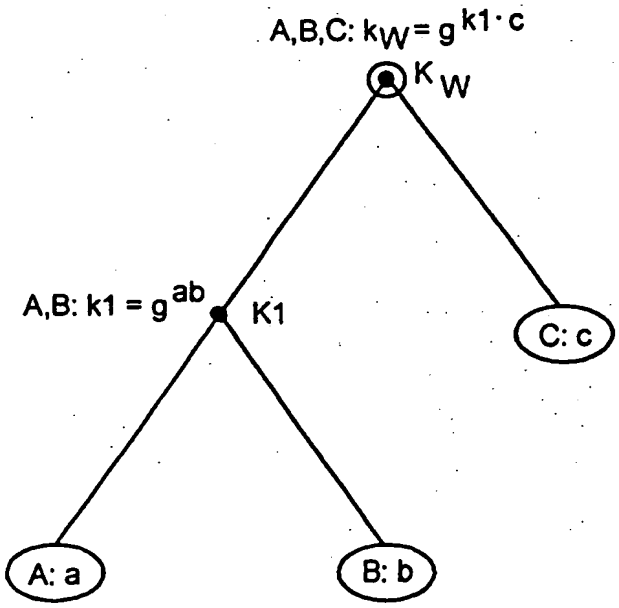
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 196 49 292 A1
DE 195 11 298 A1
US 46 61 658
US 43 09 569
EP 03 14 292 B1
JP 05327748 A.,In: Patent Abstracts of Japan;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zum Etablieren eines gemeinsamen krytografischen Schlüssels für n Teilnehmer

(57) Das Verfahren soll so ausgebildet werden, daß auch nach dem Etablieren des Gruppenschlüssels ohne großen Aufwand Teilnehmer aus dem Schlüsselverzeichnis gelöscht oder hinzugefügt werden können.
Erfindungsgemäß wird jedem der n Teilnehmer (I) jeweils ein Blatt eines binär strukturierten Baumes, der genau n Blätter und die Tiefe $[\log_2 n]$ besitzt, zugeordnet. Für jeden Teilnehmer (I), der ein Geheimnis (i) generiert und dem Blatt des Baumes zugeordnet wird, wird auch der jeweilige Teilnehmer (I) zugeordnet. Nacheinander werden in Richtung der Baumwurzel für alle Knoten (K) des Baumes Geheimnisse etabliert, wobei immer zwei bereits bekannte Geheimnisse über das DH-Verfahren zu einem neuen gemeinsamen Geheimnis zusammengefaßt werden. Der letzte Knoten K_w enthält den gemeinsamen Schlüssel aller n Teilnehmer.
Das erfindungsgemäße Verfahren läßt sich vorteilhaft zur Erzeugung eines kryptografischen Schlüssels für eine Gruppe von Teilnehmern einsetzen, deren Teilnehmerzahl Änderungen unterworfen ist.



DE 198 47 941 A 1

Beschreibung

Das erfindungsgemäße Verfahren dient der Erzeugung und dem Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer zur Gewährleistung der Geheimhaltung von Nachrichten, die über unsichere Kommunikationskanäle ausschließlich an die n Teilnehmer übertragen werden sollen.

Zum Schutz der Vertraulichkeit und Integrität der Kommunikation zwischen zwei oder mehr Personen werden die Mechanismen der Verschlüsselung und Authentisierung eingesetzt. Diese erfordern allerdings das Vorhandensein einer gemeinsamen Information bei allen Teilnehmern. Diese gemeinsame Information wird als kryptographischer Schlüssel bezeichnet.

Ein bekanntes Verfahren zum Etablieren eines gemeinsamen Schlüssels über unsichere Kommunikationskanäle ist das Verfahren von Diffie und Hellman (DH-Verfahren vergleiche W. Diffie und M. Heliman, New Directions in Cryptography, IEEETransactions, on Information Theory, IT-22(6): 644–654, November 1976).

Grundlage des Diffie-Hellmann-Schlüsselaustauschs (DH76) ist die Tatsache, daß es praktisch unmöglich ist, Logarithmen modulo einer großen Primzahl p zu berechnen. Dies machen sich Alice und Bob in dem unten abgebildeten Beispiel zunutze, indem sie jeweils eine Zahl x bzw. y kleiner als p (und teilerfremd zu p-1) geheim wählen. Dann senden sie sich (nacheinander oder gleichzeitig) die x-te (bzw. y-te) Potenz einer öffentlich bekannten Zahl α zu. Aus den empfangenen Potenzen können sie durch erneutes Potenzieren mit x bzw. y einen gemeinsamen Schlüssel K: = α^{xy} berechnen. Ein Angreifer, der nur α^x und α^y sieht, kann daraus K nicht berechnen. (Die einzige heute bekannte Methode dazu bestünde darin, zunächst den Logarithmus z. B. von α^x zur Basis α modulo p zu berechnen und dann α^y damit zu potenzieren.)

Beispiel für Diffie-Hellmann-Schlüsselaustausch

Alice		Bob
Wählt x geheim	α^x →	
	← α^y	
Bildet K: = $(\alpha^y)^x = \alpha^{xy}$		Bildet K: =$(\alpha^x)^y = \alpha^{xy}$

Das Problem bei dem im Beispiel beschriebenen DH-Schlüsselaustausch besteht darin, daß Alice nicht weiß, ob sie tatsächlich mit Bob oder mit einem Betrüger kommuniziert. In IPSec wird dieses Problem durch den Einsatz von Public-Key-Zertifikaten gelöst, in denen durch eine vertrauenswürdige Instanz die Identität eines Teilnehmers mit einem öffentlichen Schlüssel verknüpft wird. Dadurch wird die Identität eines Gesprächspartners überprüfbar.

Der DH-Schlüsselaustausch kann auch mit anderen mathematischen Strukturen realisiert werden, z. B. mit endlichen Körpern GF(2^n) oder elliptischen Kurven. Mit diesen Alternativen kann man die Performance verbessern. Dieses Verfahren ist allerdings nur zur Vereinbarung eines Schlüssels zwischen zwei Teilnehmern geeignet.

Es wurden verschiedene Versuche unternommen, das DH-Verfahren auf drei oder mehr Teilnehmer zu erweitern (Gruppen DH). (Einen Überblick über den Stand der Technik bietet M. Steiner, G. Tsudik, M. Waidner, Diflie-Hellman Key Distribution Extended to Group Communication. Proc. 3rd ACM Conference on Computer and Communications Security, März 1996, Neu Delhi, Indien.)

Eine Erweiterung des DH-Verfahren auf drei Teilnehmer A, B und C wird z. B. durch nachfolgende Tabelle beschrieben. (Berechnung jeweils mod p):

	A → B	B → C	C → A
1. Runde	g^a	g^b	g^c
2. Runde	g^{ca}	g^{ab}	g^{bc}

Nach Durchführung dieser beiden Runden kann jeder der drei Teilnehmer den geheimen Schlüssel g^{abc} mod p berechnen.

Bei allen diesen Erweiterungen tritt mindestens eines der drei folgenden Probleme auf:

- Die Teilnehmer müssen in einer bestimmten Art und Weise geordnet sein, im obigen Beispiel z. B. als Kreis.
- Die Teilnehmer haben gegenüber der Zentrale keinen Einfluß auf die Auswahl des Schlüssels.
- Die Rundenzahl ist abhängig von der Teilnehmerzahl

Ein weiteres Verfahren zum gemeinsamen Etablieren eines Schlüssels ist aus DE 195 38 385.0 bekannt. Bei diesem Verfahren muß die Zentrale allerdings die geheimen Schlüssel der Teilnehmer kennen.

Weiterhin ist eine Lösung aus Burmester, Desmedt, A secure and efficient conference key distribution system, Proc.

EUROCRYPT'94, Springer LNCS, Berlin 1994 bekannt, bei der zwei Runden zur Generierung des Schlüssels benötigt werden, wobei in der zweiten Runde durch die Zentrale für n Teilnehmer n Nachrichten der Länge p = ca. 1000 Bit gesendet werden müssen.

Bekannt ist auch ein als (n,t)-Threshold-Verfahren bezeichnetes kryptografisches Verfahren. Mit einem (n,t)-Threshold-Verfahren kann man einen Schlüssel k so in t Teile, die shadows genannt werden, zerlegen, daß dieser Schlüssel k aus je n der t shadows rekonstruiert werden kann (vgl. Beutelspacher, Schwenk, Wolfenstetter: Moderne verfahren der Kryptographie (2. Auflage), Vieweg Verlag, Wiesbaden 1998).

Das vorliegende Verfahren soll das Etablieren eines gemeinsamen Gruppenschlüssels zwischen einer Zentrale und einer Gruppe von n Teilnehmern ermöglichen. Das Verfahren soll so ausgebildet werden, daß auch nach dem Etablieren des Gruppenschlüssels ohne großen Aufwand Teilnehmer aus dem Schlüsselverzeichnis gelöscht oder hinzugefügt werden können.

Die Aufgabenstellung wird durch eine Verfahren gelöst, bei welchem das Etablieren eines Gruppenschlüssels mit Hilfe einer Baumstruktur vorgenommen wird. Erfindungsgemäß wird dazu die Anzahl der an der Schlüsselvereinbarung beteiligten Teilnehmer n als binärer Baum mit n Blättern darstellen. Für jede natürliche Zahl n gibt es ein oder mehr Darstellungen dieser Art. Die Anzahl der Blätter ist dabei mit der Anzahl der in das Verfahren einbezogenen Teilnehmer identisch. Das bedeutet, daß einer Anzahl von n Teilnehmern eine Anzahl von n Blätter eines binären Baumes mit der Tiefe $[\log_2 n]$ zugeordnet ist.

Fig. 1 zeigt das Wirkprinzip des erfindungsgemäßen Verfahrens anhand der Baumstruktur einer Schlüsselvereinbarung für drei Teilnehmer A, B, C.

Um einen gemeinsamen Schlüssel zu etablieren, gehen die Teilnehmer A, B und C wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit nach dem Zufallsprinzip generierten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1 = g^{ab} \bmod p$, der dem gemeinsamen Knoten K1 zugeordnet wird.
- Teilnehmer A und B auf der einen und Teilnehmer C auf der anderen Seite führen ein zweites DH-Verfahren durch, welches auf dem gemeinsamen Schlüssel k1 der Teilnehmer A und B und auf einer nach dem Zufallsprinzip generierten Zahl c des Teilnehmers C beruht. Das Ergebnis ist der gemeinsame Schlüssel $k = g^{k1 \cdot c} \bmod p$, der der Wurzel des Baumes K_W zugeordnet wird.

Das erfindungsgemäße Verfahren wird anhand von Ausführungsbeispielen näher erläutert.

In **Fig.** 2 ist die Baumstruktur für eine Schlüsselvereinbarung für vier Teilnehmer A, B, C und D dargestellt.

Fig. 3 zeigt die Baumstruktur einer Schlüsselvereinbarung für 5 Teilnehmer A, B, C, D und E.

Fig. 4 zeigt, ausgehend von einer bereits bestehenden Baumstruktur nach **Fig.** 2, ein Beispiel für die Erweiterung der Baumstruktur um einen Teilnehmer.

Fig. 5 zeigt, ausgehend von einer bereits bestehenden Baumstruktur nach **Fig.** 2, das Entfernen/Löschen eines Teilnehmers aus der Baumstruktur.

Nachfolgend wird anhand von **Fig.** 2 ein Beispiel einer Schlüsselvereinbarung für vier Teilnehmer A, B, C und D beschrieben:

Um einen gemeinsamen Schlüssel für vier Teilnehmer (**Fig.** 2) zu etablieren, gehen Teilnehmer A, B, C und D wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit nach dem Zufallsprinzip generierten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1 = g^{ab} \bmod p$.
- Teilnehmer C und D führen ein DH-Verfahren mit zufällig gewählten Zahlen c und d durch. Sie erhalten den gemeinsamen Schlüssel $k2 = g^{cd} \bmod p$.
- Teilnehmer A und B auf der einen und Teilnehmer C und D auf der anderen Seite führen gemeinsam ein zweites DH-Verfahren durch, in welches von Teilnehmer A und B der Schlüssel k1 und von Teilnehmer C und D der Schlüssel k2 einbezogen werden. Das Ergebnis ist der gemeinsame Schlüssel $k_w = g^{k1 \cdot k2} \bmod p$, welcher der Wurzel des Baumes K_W zugeordnet ist.

Nachfolgend wird anhand von **Fig.** 3 ein Beispiel einer Schlüsselvereinbarung für fünf Teilnehmer A, B, C, D, und E beschrieben:

Um einen gemeinsamen Schlüssel zu etablieren, gehen die Teilnehmer A, B, C, D und E wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit zufällig gewählten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1 = g^{ab} \bmod p$.
- Teilnehmer C und D führen ein DH-Verfahren mit zufällig gewählten Zahlen c und d durch. Sie erhalten den gemeinsamen Schlüssel $k2 = g^{cd} \bmod p$.
- Teilnehmer A und B auf der einen Seite und Teilnehmer C und D auf der anderen Seite führen gemeinsam ein zweites DH-Verfahren durch, in welches von Teilnehmer A und B der gemeinsame Schlüssel k1 und von Teilnehmer C und D der gemeinsame Schlüssel k2 einbezogen werden. Das Ergebnis ist ein gemeinsamer Schlüssel $k3 = g^{k1 \cdot k2} \bmod p$ für die Teilnehmer A, B, C und D.
- Die Teilnehmer A, B, C und D auf der einen Seite und der Teilnehmer E auf der anderen Seite führen ein drittes DH-Verfahren durch, in welches der gemeinsame Schlüssel k3 der Teilnehmer A, B, C und D und eine für den Teilnehmer E generierte Zufallszahl e einbezogen werden. Das Ergebnis ist der gemeinsame Schlüssel $kw = g^{k3 \cdot e} \bmod p$, der der Wurzel des Baumes K_W zugeordnet ist.

Aufgrund der Struktur des erfindungsgemäßen Verfahrens ist es möglich, neue Teilnehmer mit einzubeziehen bzw. einzelne Teilnehmer auszuschließen, ohne das ganze Verfahren für jeden Teilnehmer noch einmal durchführen zu müs-

sen.

Das Einfügen eines neuen Teilnehmers wird anhand einer Baumstruktur mit vier Teilnehmern nach **Fig.** 4 näher erläutert: Ausgangssituation ist dabei eine Baumstruktur entsprechend **Fig.** 2 in welche eine neuer Teilnehmer bei Blatt B eingefügt werden soll. Bei Hinzunahme eines neuen Teilnehmers in eine bereits bestehende Baumstruktur, die über ein gemeinsames Geheimnis verfügt, werden zum Etablieren eines neuen gemeinsamen Schlüssels für n+1 Teilnehmer an einer geeigneten Stelle des binären Baumes (Blatt B vorgegeben) zwei neue Blätter B1 und B2 angefügt. Der neue Baum besitzt dann n+1 Blätter und die Tiefe $[\log_2(n+1)]$. Der bisher dem Blatt B zugeordnete Teilnehmer wird einem der neue Blätter B1 zugeordnet. Der neue Teilnehmer wird dem anderen noch freien Blatt B2 zugeordnet. Das bisherige Blatt B wird zu einem Knoten K1 für die Blätter B1 und B2. Ausgehend von den neuen Blättern B1 und B2 werden bis hin zur Wurzel des Baumes nur in den Knoten K neue Geheimnisse etabliert, die im Rahmen der Baumstruktur auf dem Weg von den neuen Blättern B1 und B2 zur Wurzel des Baumes K_W liegen. Das sind im konkreten Fall die Knoten K1, K2 und K_W.

Ist die Anzahl der Teilnehmer eine Zweierpotenz, so erhöht sich die Tiefe des Baumes durch diesen Vorgang um 1 (vgl. vorhergehendes Beispiel). Ist die Anzahl der Teilnehmer keine Zweierpotenz, so kann durch geschickte Wahl des aufzuteilenden Blattes eine Vergrößerung der Tiefe vermieden werden, wie das folgende Beispiel zeigt:

Um beispielsweise einen vierten Teilnehmer zu drei Teilnehmern hinzuzufügen, geht man (ausgehend von der Situation nach **Fig.** 1) wie folgt vor:

- Teilnehmer C führt mit dem neu hinzugekommenen Teilnehmer D ein DH-Verfahren mit zufällig generierten Zahlen c und d durch (c sollte sich von dem vorher gewählten c unterscheiden, dies muß aber nicht der Fall sein). Das Ergebnis ist $k2 = g^{c \cdot d} \bmod p$.
- Teilnehmer A und Teilnehmer B auf der einen und Teilnehmer C und D auf der anderen Seite führen ein DH-Verfahren mit den Werten k1 und k2 durch. Das Ergebnis ist $k = g^{k1 \cdot k2'} \bmod p$.

Bei einer derartigen Konfiguration müssen die Teilnehmer A und B keinen neuen Schlüsseltausch durchführen. Generell müssen nur die Geheimnisse neu vereinbart werden, die im zugehörigen Baum auf dem Weg vom Blatt des neuen Teilnehmers zur Wurzel K_W liegen.

Das Ausschließen bzw. Löschen eines Teilnehmers wird anhand einer Baumstruktur mit vier Teilnehmern anhand von **Fig.** 5 näher erläutert: Ausgangssituation ist dabei eine Baumstruktur entsprechend **Fig.** 2, aus der Teilnehmer B entfernt werden soll.

Beim Ausschließen bzw. beim Löschen eines Teilnehmers B aus einer bereits bestehenden Baumstruktur, die über ein gemeinsames Geheimnis verfügt, werden wie in **Fig.** 5 ausgeführt, sowohl das Blatt des zu entfernenden Teilnehmers B als auch das Blatt des dem gleichen gemeinsamen Knoten K1 zugeordneten Teilnehmers A entfernt. Der gemeinsame Knoten K1 wird zum neuen Blatt A' des in der Baumstruktur verbleibenden Teilnehmers A. Ausgehend von den Blättern des Baumes bis zur Wurzel K_W werden nur in den Knoten K neue Geheimnisse etabliert, die vom neuen Blatt A' im Rahmen der Baumstruktur in Richtung Wurzel K_W unmittelbar tangiert werden. Das ist im konkreten Fall nur der Wurzelknoten K_W. Bei einer derartigen Konfiguration müssen die Teilnehmer C und D keinen neuen Schlüsseltausch durchführen. Generell müssen auch hier nur die Geheimnisse neu vereinbart werden, die im zugehörigen Baum auf dem Weg vom Blatt des Partners des entfernten Teilnehmers zur Wurzel liegen.

Das Verfahren kann in vielfacher Hinsicht zweckmäßig weiter ausgestaltet werden:

Für die Bildung der diskreten Exponentialfunktion $x \longrightarrow g^x$ bietet sich beispielsweise die Verwendung anderer Gruppen an.

Beim Hinzufügen oder Entfernen eines Teilnehmers kann beispielsweise vereinbart werden, daß für die notwendigen neuen Durchführungen des DH-Verfahrens nicht die alten Geheimnisse, sondern das Ergebnis einer (evtl. randomisierten) Einwegfunktion verwendet wird.

Patentansprüche

1. Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer unter Anwendung des DH-Verfahrens, **dadurch gekennzeichnet,**
   - daß jedem der n Teilnehmer (I) jeweils ein Blatt eines binär strukturierten Baumes, der genau n Blätter und die Tiefe $[\log_2 n]$ besitzt, zugeordnet wird,
   - daß für jeden Teilnehmer (I) ein Geheimnis (i) generiert und dem Blatt des Baumes zugeordnet wird, dem auch der jeweilige Teilnehmer (I) zugeordnet ist,
   - daß nacheinander in Richtung der Baumwurzel für alle Knoten (K) des Baumes Geheimnisse etabliert werden, wobei ausgehend von den Blättern entsprechend der festgelegten Baumstruktur über die gesamte Hierarchie der Baumstruktur immer zwei bereits bekannte Geheimnisse über das DH-Verfahren zu einem neuen gemeinsamen Geheimnis zusammengefaßt und einem gemeinsamen Knoten (K) zu geordnet werden, so daß der letzte Knoten K_W und damit die Baumwurzel, als Geheimnis den gemeinsamen Schlüssel aller n Teilnehmer enthält.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,
   - daß bei Aufnahme eines neuen Teilnehmers in eine bestehende Baumstruktur, die bereits über ein gemeinsames Geheimnis verfügt, zum Etablieren eines gemeinsamen Schlüssel für n+1 Teilnehmer an geeigneter Stelle des binären Baumes einem Blatt (B) als Nachfolger zwei neue Blätter (B1 und B2) angefügt werden, so daß der neue Baum genau n+1 Blätter und die Tiefe $[\log_2(n+1)]$ besitzt,
   - daß der dem bisherigen Blatt (B) zugeordnete Teilnehmer und der neue Teilnehmer jeweils einem der neuen Blätter (B1; B2) zugeordnet werden, wobei das bisherige Blatt B zu einem gemeinsamen Knoten für die neuen Blätter (B1; B2) wird,

– daß ausgehend von den neuen Blättern (B1; B2) bis zur Wurzel des Baumes nur in den Knoten neue Geheimnisse etabliert werden, die im Rahmen der Baumstruktur auf dem Weg von den Blättern B1 und B2 zur Baumwurzel liegen.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet,
   – daß bei Ausschließung eines Teilnehmers (B) aus einer bereits bestehenden Baumstruktur die bereits über ein Geheimnis verfügt, sowohl das Blatt des zu entfernen den Teilnehmers (B), als auch daß Blatt des dem gleichen gemeinsamen Knoten zugeordneten Teilnehmers (A) entfernt werden,
   – daß der gemeinsame Knoten zum Blatt des nicht zu entfernende Teilnehmers A wird, und daß ausgehend von den Blättern des Baumes bis zur Wurzel nur in den Knoten neue Geheimnisse etabliert werden, die im Rahmen der Baumstruktur auf dem Weg vom neuen Blatt (A) zur Baumwurzel liegen.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 198 47 941 A1
Int. Cl.[7]: H 04 L 9/30
Offenlegungstag: 13. April 2000

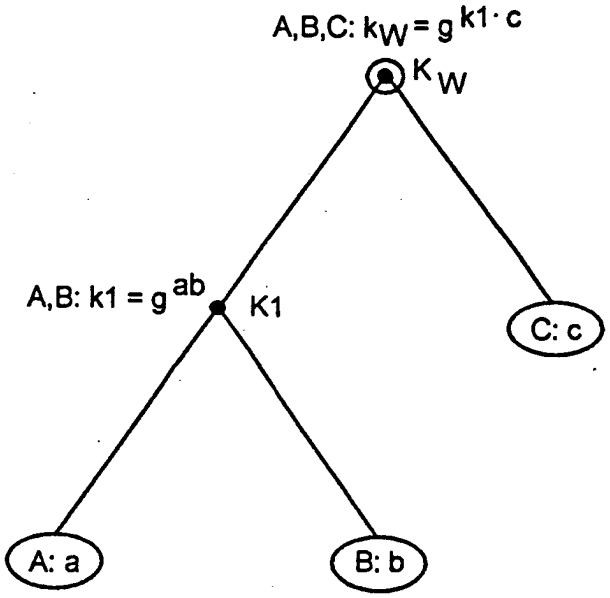


Fig. 1

Nummer: DE 198 47 941 A1
Int. Cl.[7]: H 04 L 9/30
Offenlegungstag: 13. April 2000

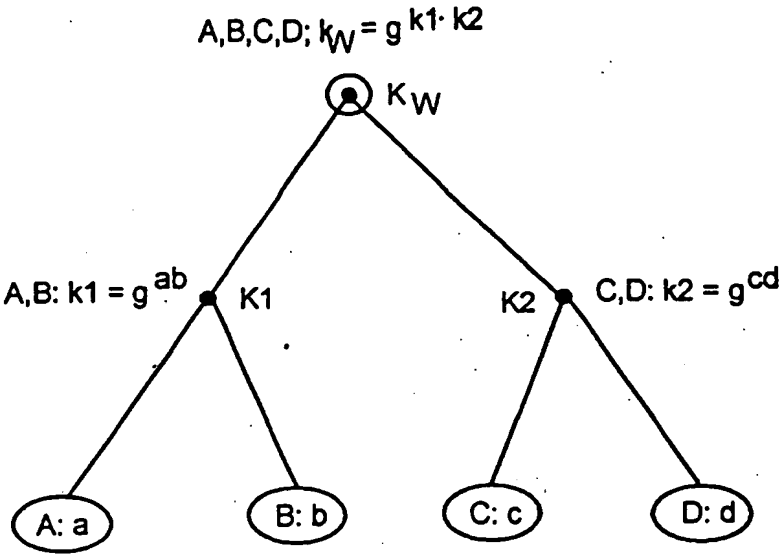


Fig. 2

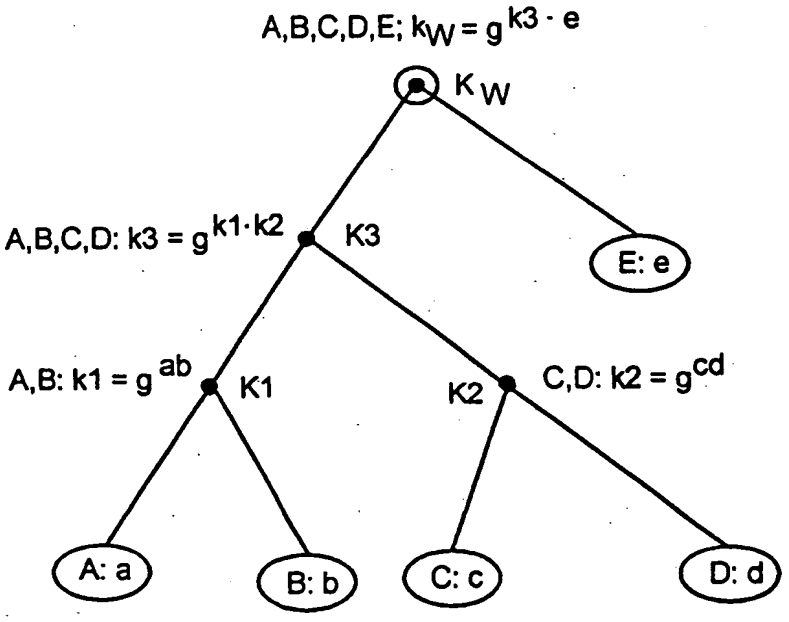


Fig. 3

Nummer: DE 198 47 941 A1
Int. Cl.[7]: H 04 L 9/30
Offenlegungstag: 13. April 2000

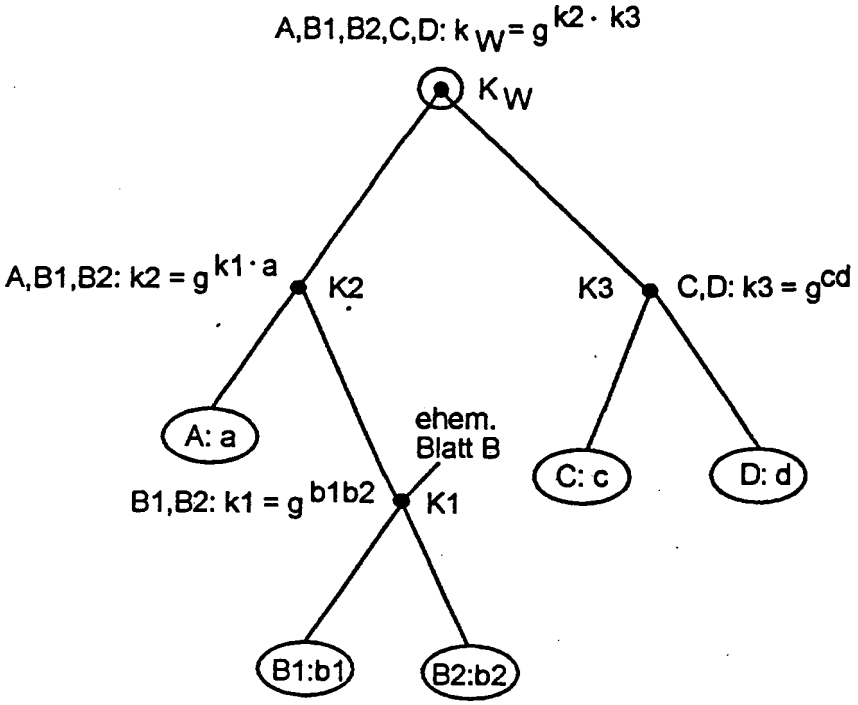


Fig. 4

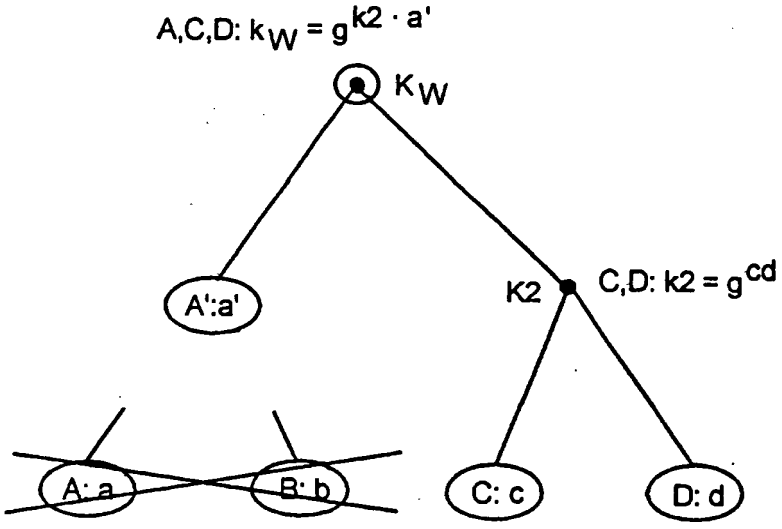


Fig. 5